

Cover Sheet for Proposals <i>(All sections must be completed)</i>		
Name of Capital Programme:	e-Research: e-Infrastructure	
Name of Lead Institution:	Cardiff University	
Name of Proposed Project:	Self-Protecting Information for De-perimeterised Electronic Relationships (SPIDER)	
Name(s) of Project Partner(s):	N/A	
Full Contact Details for Primary Contact:		
Name: Jeremy Hilton		
Position: Lecturer, School of Computer Science		
Email: Jeremy.hilton@cs.cardiff.ac.uk		
Address: Cardiff School of Computer Science, Queens Building, 5 The Parade, Roath, Cardiff, CF24 3AA		
Tel: 07753 816596		
Fax: 029 2987 4598		
Length of Project:	1 year	
Project Start Date:	Beginning January 2008	Project End Date: End December 2008
Total Funding Requested from JISC: £109,899 (see project budget)		
Funding Broken Down over Financial Years (Apr–Mar):		
	Jan08 – Mar08	Apr08 – Dec08
	£27475	£82424
Total Institutional Contributions: £3000 for equipment, plus £7000 for senior INSRV staff time		
Outline Project Description		
The aim of this project is to produce a mechanism for the secure sharing of information at a finer level of granularity than is currently possible.		
The project will:-		
<ul style="list-style-type: none"> • research and analyse the associated risks for information sharing in collaborative distributed environments using sample medical research data • take the set of requirements and implement a solution that considers these requirements • improve the understanding of the collaborative reworking community as to how information exchange could be greatly improved by providing much finer grained access controls 		
I have looked at the example FOI form at Appendix A and included an FOI form in the attached bid (Tick Box)	YES	NO
I have read the Circular and associated Terms and Conditions of Grant at Appendix B (Tick Box)	YES	NO

FOI Withheld Information Form

We would like JISC to consider withholding the following sections or paragraphs from disclosure, should the contents of this proposal be requested under the Freedom of Information Act, or if we are successful in our bid for funding and our project proposal is made available on JISC's website.

We acknowledge that the FOI Withheld Information Form is of indicative value only and that JISC may nevertheless be obliged to disclose this information in accordance with the requirements of the Act. We acknowledge that the final decision on disclosure rests with JISC.

Section / Paragraph No.	Relevant exemption from disclosure under FOI	Justification
Nil		

Self-Protecting Information for De-perimeterised Electronic Relationships (SPIDER)

1. Appropriateness and Fit to Programme Objectives and Overall Value to the JISC Community

1.1 Project Description

Collaborative working between multiple organisations will always require some level of information sharing and exchange. A significant amount of information belonging to an organisation will have an associated value for which appropriate protection mechanisms must be put in place in order to prevent the exposure or loss of that information. The emergence of Grid computing and Service-Oriented Architectures have led to the increasing adoption of dynamically formed, collaborative working groups known as Virtual Organisations (VOs). These Virtual Organisations (VOs), as defined in [FoKe03]¹ and [FoKT01]², provide strong motivation for investigation into the infrastructure, and in particular the security necessary to protect the information and resources shared within a VO, both while resident on local machines and when allowed to move beyond the secure boundary of a local organisational network perimeter and into the realm of the distributed VO.

Previous research in the area of access control approaches to shared information to date such as VOMS, PERMIS, ShARPE and iRODS have focused on the protection of information resources as an entity within the secure system boundary, for example, an entire classified document; access is either granted or denied using system-level access controls, or Digital Rights Management (DRM) techniques on the entity. This approach often has two major drawbacks:

- It hinders information sharing to some extent due to its limited granularity. That is, information sharing, and as a result collaborative working, is not being allowed to reach its maximum potential because large amounts of information cannot be shared due to small amounts of higher-level sensitive content within the resource raising the overall classification of the resource.
- With current DRM and system-level controls that can control access to information to some extent *after* the information has been allowed to move beyond an organisation's access control perimeter, the access control policy is permanent and cannot be modified by the owner of the information. However, there may be a change in the controls required to protect a resource, for example, the VO working group may disperse or the VO community may be changed, thus wishing to deny access to information previously shared.

This project aims to address both drawbacks by first of all designing and implementing an approach to access control which removes the fixed boundaries around the whole information resource, and places boundaries just around the sensitive content within the resource, thereby putting part of the access control policy within the information itself, and allowing the access restrictions to apply to not only the entire resource (as currently achieved), but also the content within. This has the potential to allow the sensitive content to be strictly controlled, while the rest of the information in the resource can be made publicly available. Different views of a resource can be created for varying levels of access control.

The second phase of the project addresses the implementation of modifiable policy, even on resources that have been stored on media outside the control of the system access control perimeter. The proposed work will review and build on current and emerging standards/approaches to Information Security that define policy and place access control restriction criteria with the information resource itself, instead of the common approach which relies on centrally controlled access to information contained within a finite perimeter (e.g. a company network).

¹ [FoKe03] Foster, I., Kesselman, C., The Grid 2: blueprint for a new computing infrastructure, 2nd Ed, San Francisco, Calif.: Morgan Kaufman, 2003

² [FoKT01] Foster, I., Kesselman, C. Tuecke, S., The Anatomy of the Grid, Enabling Scalable Virtual Organisations. Intl J. Supercomputer Applications, 15(3), 2001

1.2 Aim and Objectives

The aim of this project is to produce a mechanism for the secure sharing of information at a finer level of granularity than is currently possible. As such, this will create a contribution of understanding and solution to both the academic and commercial research and development and collaborative working communities in line with the e-Research Federated Tools and services theme of the JISC call, meeting the anticipated outcomes of a broader and more effective understanding and use of e-Infrastructure with enhanced security. Being a Welsh establishment it is also important to us that we assist in the promotion of research capacity and development of technologies for e-Research as defined by the Welsh Assembly Government's strategy for the HE sector.

The first objective is to research and analyse the associated risks for information sharing in collaborative distributed environments using some sample medical research data made available from the initial research of the CU led PET Scanner project, scheduled to be completed in 2009. Only by understanding the risk can there be a suggestion of the controls required to manage the risk, and from there the technical controls necessary can be implemented. While aiming to redefine the security requirements for VO environments, the project team are not new to the domain and are aware that technologies such as VOMS, PERMIS, ShARPE and iRODS for access control enforcement, Shibboleth for federated access management, and standards such as XACML and SAML for policy definition and decision are already available from previous research. Rather than re-inventing the wheel, the planned research and analysis will consist of an evaluation of current access control methods, technologies and standards in relation to the risk assessment carried out on the collaborative medical research environment, creating a set of requirements where current controls are lacking in comparison to the identified risks and can be built upon to improve e-Infrastructure security.

The second objective is then to take the set of requirements and implement a solution that considers these requirements, using stable open standards where appropriate, in order to provide a solution that better suits the widely distributed, expanding perimeter environments that are rapidly emerging through the adoption of VOs and collaborative working. The resulting work will provide a development to e-Infrastructure security that will allow much finer grained control over their information security and allow greater collaboration potential by increasing the amount of information that can be shared. Where previously research results or company reports were unable to be shared because they contained a small amount of information that was too sensitive to be made public, the sensitive information will be able to be classified and restricted while the rest of the information is publicly accessible.

A third objective is to improve the understanding of the collaborative working community as to how information exchange could be greatly improved by providing much finer grained access controls. The case study of testing the infrastructure with medical research data will provide a clear understanding of the technology and a use case for data access management that can be disseminated to the research communities through workshops and requests for comment to give them a better understanding of the gain in collaborative research potential that this level of fine grained control over their research information can provide. For future sustainability this solution can be built upon to production level and integrated into existing commercial enterprise architectures.

During CU's previous JISC funded projects, a high degree of time and energy has been given to collaboration with other projects and the community at large, with project staff attending JISC project meetings and attending and often speaking at both national and international events. This is important to us in our effort to establish ourselves within the relevant research domain and to share research views with other likeminded organisations. This project will aim to continue in this vein.

2. Quality of Proposal and Robustness of Workplan

The project will be managed by the core project team at Cardiff University consisting of members of the School of Computer Science (COMSC) and the department of Information Services (INSRV).

Most of the work will be carried out by the Principal Investigator and Senior Researcher in COMSC. The Senior Researcher has previous experience in developing and managing projects funded by DTI, EPSRC and OMII and has been actively researching and developing software very closely linked to this work over the past 18 months. Members of the project team from INSRV have a good deal of experience with

managing JISC projects from their involvement with the ASMIMA project, The Identity Project, and Project CUCKOO (all JISC funded), and will use this experience to help guide the project.

2.1 Outline Project Timetable

The following section outlines the proposed research and development as a detailed set of work packages. The project schedule presented as a Gantt chart can be found in Annex A on page 10 of this proposal.

Work Package 1

The initial stage of the project will be to research current standards and technologies for data-level protection, the use of information classification schemes, and definition and enforcement of policy-controlled access to information – both at system level and the human readable level. The project team already has a research website and a domain will be set up on that site for the findings of this project.

Deliverables

- Project paper and report on findings
- Post findings to project website

Work Package 2

It is then proposed to undertake a risk assessment of the healthcare collaborative research environment in line with the PET scanner project currently underway at CU in order to understand the information security issues. An analysis of the risk assessment will identify the issues that can be effectively managed by existing security methods and identify those issues not addressed.

Deliverables

- Requirements specification for access control technology in VO research environments document
- Update website with this document

Work Package 3

Early on in the project it will be necessary to develop a policy notation to enable the declaration of information protection requirements that is human and machine readable. This ensures the implementation of system-level security controls through policy bound to the data element. It is required early so that system implementation can begin early in the project cycle. Detailed policy can be specified in this notation later in the project to test the application of specific controls.

Deliverables

- Policy notation document
- Policy enforcement requirements specification

Work Package 4

Based on the security requirements specifications identified in WP 2 and 3, an information classification scheme and related protection needs will be defined. These needs will have access control policies defined, applicable both to human users and machine-readable system security policies. Following this study, a specification for a VO Security System will be defined. This will include a policy notation common to the platform and data elements.

Deliverables

- Information classification scheme requirements and definition document
- Access control policy requirements and definition document
- VO security system architecture defined

Work Package 5

Whilst the system is being implemented (see WP 6), it is proposed to explore the transferability of the information classification scheme and associated controls to the medical research environment, particularly with respect to medical research results by applying it to a sample set of data from the PET scanner project. The aim is to both test the usability of the results as well as to develop a generic scheme that can be used by any organisation in a VO processing sensitive data.

Deliverables

- Conference paper on application of the information classification scheme and related controls to medical research information

Work Package 6

The system specification will be implemented using a service-oriented architecture, utilising web services, policy definition and user identity standards and related technologies, and latest security infrastructure. The system will be developed with an underlying distributed architecture to provide an alternative to the more common approach of centralised user management and security control.

Deliverables

- Conference paper on the system architecture and comparison to existing architectures that do need meet the requirements of collaborative VO information sharing to such a fine granularity.
- Software implementation of the proposed system architecture for demonstration and dissemination.

Work Package 7

The implementation of the technical solution would then be installed onto the test-bed machines to provide a live test scenario and initial performance results. By setting up several back-end machines hosting various information resources, all of which have the access control policy applied to them, the access control mechanisms can be enforced by attempting to access the resources through the software installed on the client machines. UCISA and ENISA will be invited to submit information of their own to the test-bed to provide additional results and proof of concept. We also consider testing the robustness of the prototype, in the first instance, by offering a challenge with CU's School of Computer Science to see if anybody can crack the security. Subsequently we may offer the same challenge to members of the Jericho Forum. The software will be fully documented with FAQ, installation guide and distributed with the initial test results. Guidance will be taken from the Open Source Maturity Model, and the senior researcher on the project has previous experience with the quality assured development of software for the OMII.

Deliverables

- Journal paper on the complete solution to include the initial research, analysis and risk assessment of VO research environments, information classification scheme and policy notation, and software implementation
- Release (under licence) of the first version of the software including documentation
- Presentation/Demonstration of the software internally at CU, to UCISA, to the Jericho Forum members, and to ENISA.
- Report on future development requirements and bugs

Work Package 8

The final work package will see the end of the project, but after the various papers and particularly, the demonstrations to CU, UCISA, Jericho Forum and ENISA, the project will be sustainable through integration into any one (or more) of the enterprise architectures of these organisations or by sale under licence to other organisations. The final report to JISC will be the end of this funded work, but the agenda at CU is to push the resulting theories and software into the academic and commercial domains.

Deliverables

- Conference and Journal papers, once published will be published on the project web site
- Final Project Report
- Publication of all related work to website (ongoing)

2.2 Project Governance and Evaluation

Though this is an internal CU project, it is cross-disciplinary and as we wish to implement the results, the approach developed must be capable of implementation within the CU infrastructure. Consequently we will establish a steering committee with members from Corporate Compliance, Information Services and Computer Science. Due to the anticipated benefit to UCISA, a UCISA expert will also be invited to join the Steering Committee. We would also seek an appropriate input from JISC in an advisory capacity, or as a member of the steering committee.

The Steering Committee will meet at the beginning and end of the project, as well as at suitable milestones to be decided at the beginning of the project. Appropriate documentation in accordance with PRINCE 2 will be developed; the minimum being product descriptions and a full project plan, to be agreed at the first Steering Committee meeting.

2.3 Risk Assessment

Risk	Prob (1-5)	Impact (1-5)	P x I	Risk Management
Loss of core project staff	1	2	2	The CU research team have strength in depth and any loss of contribution from core project staff could be distributed to other capable staff.
Failure to get papers published	2	1	2	This is a contemporary and interesting area of research and should be relevant to upcoming conferences and journal publications. If not, the research will be disseminated through demonstration to ENISA, Jericho Forum and other interested parties, and case study reports.
Failure to find use case for proof-of-concept	1	3	3	The failure to find a use case would impact the credibility of the work as proof-of-concept could not be demonstrated. However, CU has its own internal information management infrastructure which could be used for demonstration should the failure occur
Failure to deliver suitable technical solution	1	4	4	The project would be a failure if a technical solution were not produced but regular project progress meetings and the deadlines set for publication of progressive work, along with the technical expertise and experience at CU should ensure that the deadline is adhered to and a solution produced

2.4 IPR

The deliverables produced will be made available under open source licensing arrangements. We intend to utilise the creative commons notation³.

³ <http://creativecommons.org/licenses/>

3. Engagement with the Community

3.1 Community Use

Organisations currently aiming to develop the ability to retrieve, assemble and disseminate information from multiple sources in order to support collaborative research and development; spread knowledge of best practice; and promote collaboration between organisations are ideal scenarios for demonstrating the proposed system architecture. Cardiff has links to two organisations that could be used as case studies:

- In academia, the Universities and Colleges Information Systems Association (UCISA), who have recently published a toolkit to help manage information risks within educational networks. Within the toolkit there is a recommendation for the requirement of information classification according to sensitivity, with the classification labels being used to communicate the handling and protection requirements to others. To date, there is no set of controls to enforce this. The project team includes a UCISA expert who will request the involvement of UCISA in the testing and evaluation of the solution, should the proposal be successful.
- Outside of academia, the European Network Information Security Association (ENISA) have recently commissioned members of the core project team to conduct an information risk assessment/risk management method evaluation in order to identify a set of requirement criteria for a method that would enable the assessment and management of emerging and future risks. Part of the requirement was that the method should be able to retrieve, analyse and disseminate information regarding emerging and future applications and technologies from European member states for the generation of scenarios that can be risk assessed. One of the issues arising from this work was the fact that the information would be retrieved from various sources, with some of that information being of a higher sensitivity level and as such, not available to be disseminated publicly. There are no controls currently in place to control the classification of information by sensitivity and apply controls to restrict access to sensitive content.

The development of the proposed system architecture would provide a solution that could be applied to both cases, providing a contribution to academic and commercial collaborative working environments, and through implementation into the enterprise architecture of either of these systems, or indeed CU's own, a potential route for sustainability to the project in addition to further research potential.

3.2 Evaluation mechanisms

The design of the system architecture for the proposed implementation will be based on a risk assessment of information shared within the medical collaborative research environment resulting from the initial results of the Welsh Assembly Government funded, CU managed PET scanner project. This risk assessment will identify the risks associated with working in this environment and from that a set of requirements can be derived for access control technologies in VO and other collaborative environments, two of which will be those identified as drawbacks with the current approach as stated above.

The implementation of the technical solution will be rolled out across several test-bed machines to provide a live test scenario and performance results. By setting up several back-end machines hosting various information resources, all of which have the access control policy applied to them, the access control mechanisms can be enforced by attempting to access the resources through the software installed on the client machines. UCISA and ENISA will be invited to submit information of their own to the test-bed to provide additional results and proof of concept. We also consider testing the robustness of the prototype, in the first instance, by offering a challenge with CU's School of Computer Science to see if anybody can crack the security. Subsequently we may offer the same challenge to members of the Jericho Forum.

3.3 Dissemination

Apart from the conference and journal papers that are produced in the work plans, CU has links to the UCISA, ENISA and Jericho Forum board. The project results and related software will be demonstrated to the each organisation, with particular interest to the Jericho Forum whose members are generally CIO level from large organisations. There has been previous interest from some members in the kind of solution proposed in this work and when results are demonstrated, it is expected that interest will rise and future research and commercial integration may occur.

3.4 Outcomes and Benefits

The major outcome of this project will come from the structure of its work packages. It is a bottom-up approach to a solution that takes an existing collaborative research scenario and conducts a risk assessment, analysis and requirements definition prior to the development of technical controls. This generates a belief of defensibility to any statements or requirements stated in the solution and the various reports and papers.

The nature of the project is that it has a final software deliverable which is a practical outcome that can be demonstrated to the academic and commercial communities through CU's various connections. Further outcomes from this will be a contribution to the electronic access control research field and a sustainable development plan for integrating the resulting solution into existing tools and services.

3.5 Institutional benefits

The key institutional benefit will be the ability to implement a working information classification scheme to support the CU Information Security Policy. Additionally, with fine grained access controls to information, many of the projects undertaken by CU can disseminate results in a more secure manner. Once the approach is proven, then research results and health information can be better managed with regard to privacy, data protection and confidentiality by researchers and clinicians.

4. Budget

	Year 2007/08	Year 2008/09	Full cost of project	Requested Funding
Directly Incurred Costs				
i. Staff Costs	10446	31339	41,785	34,785
ii. Travel & Subsistence (UK)	250	750	1,000	1,000
iii. Travel & Subsistence (Overseas)	750	2250	3,000	3,000
iv. New Equipment	3000	0	3,000	0
v. Recruitment/Advertising	0	0	0	0
vi. Consumables	0	0	0	0
vii. Other Costs - Transcription (Casual)	0	0	0	0
Publication Costs (Research Councils Only)	0	0	0	0
vii Audit Fees	0	0	0	0
viii. Sub-Contract/External Collaborators	3300	9900	13,200	13,200
Directly Allocated Costs				
i. Investigators Costs	2533	7599	10132	10132
ii. Advanced Research Computing	0	0	0	0
iii. Use of School Equipment	0	0	0	0
iv. Estates Costs	2753	8259	11012	11012
v. Other Directly Allocated Costs Staff	0	0	0	0
Other	0	0	0	0
Indirect Costs	8442.5	25327.5	33770	33770
Exceptions				
i. Staff - Project Studentship			0	0
ii. Other Costs			0	0
			0	0
TOTALS	11195.5	33586.5	116,899	106,899

The requested budget covers the costs of the key staff only. All other staff time and any IT equipment and support will be contribute by Information Services.

Travel costs in the UK include travel to JISC events and meetings with the community members, and conference attendance to present papers published as result of the research.

Travel costs overseas include travel to ENISA (Crete) to engage them in the evaluation and possible dissemination of the research.

5. Previous Experience of the Project Team

Cardiff University (CU) has been very active over the past two years in the analysis of protection profiles and requirements for information that is shared in distributed, collaborative research and commercial environments. The project team is made up of members with both academic and commercial backgrounds, and who specialise in both information systems and computer science domains. As such, the research motivation of the team at CU comes not only from a technical solution viewpoint, but largely from the necessity to enable a technical solution through applied risk assessment, security protection requirements and finally the relevant technical controls.

The project team have been involved in a number of other relevant research projects namely:

- DTI UK e-Science COVITE Project 2002-2004
This project was one of the early e-Science projects to implement a service-oriented approach to collaborative working by linking distributed, autonomous heterogeneous databases together using Grid services and associated security technology. Tested on the construction industry, the project enabled products and services to be sourced from multiple distributed suppliers through a single interface.
- EPSRC NaradaBrokering Project 2004-2005
In collaboration with the Community Grids Lab at Indiana University, USA, the project included the development, evaluation and testing of the NaradaBrokering distributed messaging infrastructure. The Narada substrate provides a messaging paradigm for collaboration using message oriented middleware, over TCP (blocking, non-blocking), UDP, Multicast, SSL, HTTP and HTTPS, Parallel TCP Streams, tested across international networks to machines in the UK, USA and Australia.
- Open Middleware Infrastructure Institute (OMII) MANGO Project 2004-2006
One of the major software repositories to be formed towards the end of the e-Science initiative, the OMII provide a set of tools and services that enable a middleware for collaborative working using a service-oriented architecture. The MANGO project involved utilising web service technology to develop services for job submission and monitoring, workflow creation and management, and notification and eventing services incorporating WS-Eventing. Including the setup and control of a secure communication environment using WS-Security, SSH and X509 security certificates between services and client/server.
- JISC The Identity Project 2006-2007
In collaboration with the London School of Economics and seven other partner institutions, CU led this project which aimed to research the current state of Identity Management in UK academic institutions, identifying common problems and areas of good practice. Future collaborative working between institutions will need work such as this because common definitions and standards will be required in a federated world.
- JISC ASMIMA Project 2005-2006
This project saw CU become an early adopter of Shibboleth and an expert in Federated Access Management technologies. This resulted in Cardiff becoming one of the first universities in the UK to implement a fully resilient production quality Shibboleth service for the whole institution: a good enabler of next generation collaborative working for its members.
- JISC CUCKOO Project 2007-2008
In collaboration with Kidderminster College, this project is examining and analysing existing tools for Virtual Organisations both currently available and forthcoming, for institutional use.

5.1 Project Team

Name	Job Title	Project Role(s)	% FTE	Days
Jeremy Hilton	Lecturer in School of Computer Science	Principal Investigator and Project Manager	████	44
Pete Burnap	Associate Lecturer in School of Computer Science	Senior Researcher	████	165
Anas Tawileh	Researcher	Research Assistant	████	44
Rhys Smith	Engineering Consultant	Research Assistant	████	22

David Harrison	Assistant Director – User Enablement	Steering Group and UCISA expert	■	4
Hugh Beedie	Assistant Director -Chief Technology Officer	Steering Group and technology design/ integration	■	11
Ms Ann Saalbach	Associate Director – Head of Business Information Systems	Steering Group and Service Owner. Link to Admin PSIG.	■	11
Lucy Burrow	University Records Manager	Steering Group and Corporate Compliance	■	4

We are seeking funding for the key personnel as identified below; Hilton, Burnap, Tawileh and Smith.

Jeremy Hilton

Principal Investigator. Lecturer in Information Systems. He is responsible for developing and delivering the MSc and BSc modules on Information Security within the School of Computer Science at Cardiff University. Additionally, he researches and applies knowledge on different methods of risk assessment and risk management and how they should be best applied in different organisations. A detailed understanding of realistic understanding of threats, vulnerabilities and incidents for IT-assets within different environments and usage scenarios is crucial. In addition to his research and teaching obligations, he consults in information security, has undertaken risk assessments for large and small organisations and has a particular sympathy for SMEs.

Pete Burnap

Senior Researcher. Many of the technologies currently used in commercial practice emerged from previous research in academic establishments so it is likely that academic research experience and results from working with current technologies will be remarkably useful when modelling potential future commercial risk. Pete has worked for several years in the academic research sector gaining valuable knowledge of contemporary Information Security and Network technology issues from an independent and impartial viewpoint. This has bred knowledge of IT application developments, emerging threats to performance and quality of service, privacy, policy and access control issues.

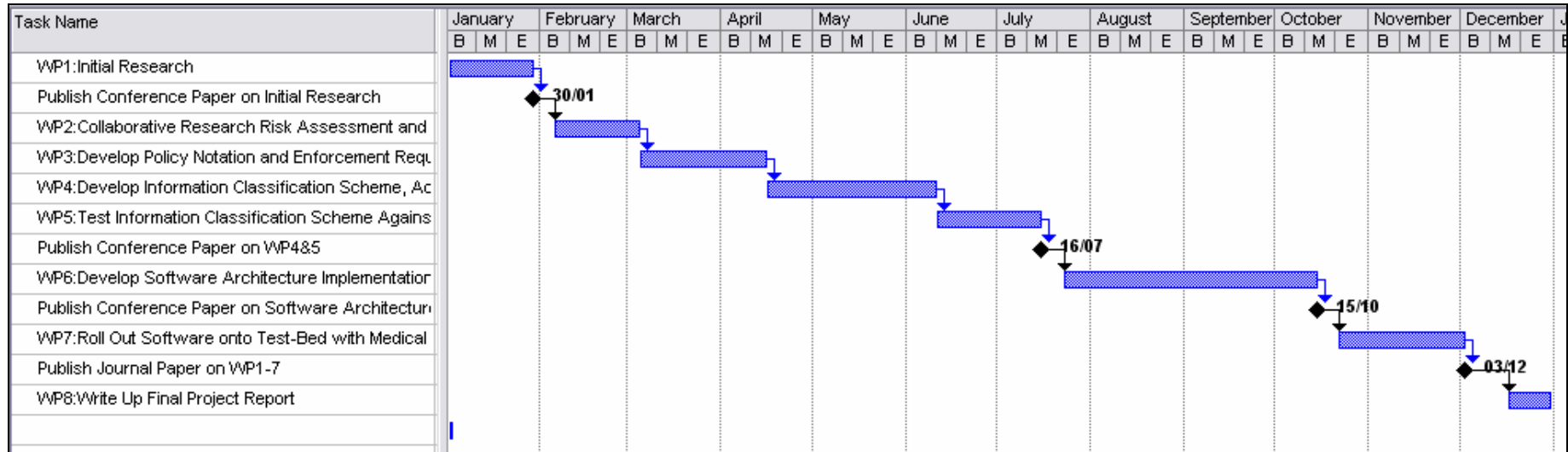
Anas Tawileh

Research Assistant. He is experienced in analysing and evaluating risks and threats to IT organisations and formulating security policies and designing information security management systems and has conducted many awareness and capacity building programmes for different organisations, including the development and dissemination of the Multi Media Training Kit (MMTK) on Wireless Community Networks for the Association of Progressive Communications. He has also participated in many awareness raising campaigns for Open Source, Creative Commons and Information Security. He has performed complete security assessments and information security management systems design for several organisation. He has good knowledge of BS7799/ISO17799.

Rhys Smith

Research Assistant. CU, Development Engineer within INSRV; was the main IT Officer for the JISC funded ASMIMA project, one of the key project personnel in the JISC funded The Identity Project, has a background in computer security and privacy, and a particular expertise in Identity Management and Federated Access Management.

Annex A – Project Plan



School of Computer Science
Head of School Professor Nick Fiddian MSc (Law) PhD (Soton) MBCS CEng CIP
Adran Cyfrifiadureg
Pennaeth Yr Ysgol Yr Athro Nick Fiddian MSc (Law) PhD (Soton) MBCS CEng CIP



Cardiff University
Queen's Buildings
5 The Parade
Roath
Cardiff CF24 3AA
Wales UK
Tel/Fon +44(0)29 2087 4812
Fax/Ffôn +44(0)29 2087 4599
www.cf.cardiff.ac.uk
Prifysgol Caerdydd
Adeiladau y Ffronhau
5 The Parade
Y Rhath
Caerdydd CF24 3AA
Cymru, Y Ddeuddeg Gyrnol

JISC
Northavon House
Coldharbour Lane
Bristol
BS16 1QD

28th September 2007

Letter of Support: Mr J Hilton

Jeremy Hilton has contributed significantly to the teaching and research activities of the Strategic Information Systems (SIS) group in the School of Computer Science at Cardiff University for the past few years – initially as an external consultant, then from summer 2005, as a new lecturer in the School. The SIS group, of which he is a key member, is responsible for creating and delivering research-led degree programmes in the area of Information Systems at both undergraduate and postgraduate levels. In addition, the group – which has a number of staff members with extensive consultancy, management and development experience of real-world complex information systems – is engaged in practice-based research collaborations with a wide variety of government and business organisations.

Jeremy's particular strength and major contribution to SIS is in the area of information security – to which he brings a wealth of insight, experience and original ideas, as his research project proposal on Self Protecting Information for De-perimeterised Electronic Relationships (SPIDER) amply demonstrates. His thinking on element-centric open systems information security and the concept of self-protecting data is at one and the same time entirely realistic and excitingly radical: it illustrates perfectly the huge potential of harnessing extensive real-world experience of complex information systems with fundamental academic research into such systems. There are some definite parallels here with the underlying context of the JISC call for Federated Tools and Services projects to explore the area of technologies for control of access to research data.

The School of Computer Science at Cardiff University received a Grade 5A in the 2001 RAE, and was chosen to host one of the eight original UK Grid Computing Centres – WeSC, the Welsh e-Science Centre. The School's research environment and facilities are fully commensurate with its Grade 5A status. New lecturing staff receive priority strategic support from the School to establish their research. Their career development at this crucial stage is facilitated by regular mentoring and formal appraisal, complemented by a wide-ranging University programme of staff development courses which are fully informed by relevant professional standards and guidelines including the Joint Statement of Research Councils on Skills Training Requirements.

Professor N J Fiddian
Head of School